



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/053,013	01/18/2002	David Kammer	035451-0170 (3708.Palm)	2103

26371 7590 10/27/2005
FOLEY & LARDNER
777 EAST WISCONSIN AVENUE
SUITE 3800
MILWAUKEE, WI 53202-5308

EXAMINER

ABEDIN, SHANTO

ART UNIT PAPER NUMBER

2136

DATE MAILED: 10/27/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

10/053,013

Applicant(s)

KAMMER ET AL.

Examiner

Shanto Abedin

Art Unit

2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 03 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☐ Responsive to communication(s) filed on 18 January 2002.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-49 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-49 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 18 January 2002 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date <u>01/18/2002</u> . | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. Claims 1-49 were presented for examination.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

2. Claims 1, 2, 11-17 are rejected under 35 U.S.C. §101 because the claimed invention is directed to non-statutory subject matter. For a subject matter to be statutory the claimed invention as a whole must accomplish a practical application. That is must produce a “useful, concrete and tangible result.” State Street, 149 F3d at 1373, 47 USPQ2d at 1601-02, MPEP § 2106.

Regarding claim 1, it was drawn to a method. All of the features and the elements of the above mentioned claim represent a mere abstract idea or manipulation of abstract idea – they lack required practical application to produce tangible result. Therefore the claim is non statutory under 35 U.S.C. 101 as not being tangible.

Regarding claims 2, 11-17 are rejected because of their dependencies on claim 1, and limitations of those claims further failed to disclose any tangible result.

Note: As best understood claims 1, 2, and 11-17 are examined, and rejected as below with all other submitted claims.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

3. Claims 1, 2, 11- 13, 15, 16 are rejected under 35 USC 102 (b) as being anticipated by Goertzel et al (Patent No: US 6308273 B1).

Regarding claim 1, Goertzel discloses a method of adjusting security for a network user node in a communication with network based upon the location of the node (Summary of the invention: network security system, and method wherein access to network resources is based on information that includes the location of connecting user; Col 5, Lines 3-57; Col 6, Lines 1-65; Col 12, Lines 11- 39; Col 17, Claim 1; Col 18, Claims 2-8; Col 19, Claim 21; Col 20, Claims 34 and 42), comprising: determining the location of a network user node (summary of the invention; Col 5, Lines 4-35; Col 12, Lines 11-39; Col 17, Claim 1; granting access to network resources by determining the location of the user) ; selecting a single level of security from a group of more than two security levels based on the determined location (Col 6, Lines 30-65; different trust/ access levels are assigned to users in different locations; Col 12, Lines 11-37; Col 17 and 18, Claims 1-8; Col 19, Claim 21); and modifying the security protection for the network user node based upon the selected level of security (Col 12, Lines 11-37; Col 20, Claims 34, and 42; restrictions in the security context are based on the access level).

Regarding claim 2, it is rejected applying as above rejecting claim 1, furthermore, Goertzel discloses network user node is a portable, handheld device having a display (Col 3, Lines 15-35, hand-held devices; Col 4, Lines 5-35, display device).

Regarding claim 11, it is rejected applying as above rejecting claim 1, furthermore, Goertzel discloses the selecting step is carried out by reference to a table of desired security modifications based upon the location of network user node (Fig 6, elements 88, 90, 92 , and 94); Col 6, lines 51-65; Col 19, claim 21; Goertzel teaches a table of access level permitted based on user location in intranet or extranet).

Regarding claim 12, it is rejected applying as above rejecting claim 11, furthermore, Goertzel discloses security levels are provided by the user of the network user node for a variety of

locations (Col 1, lines 10-65; remote access server, Internet, and mobile users; Col 5, lines 11-55; Col 6, lines 51-65; Intranet and extranet users in different locations, access levels assigned depending on user locations).

Regarding claim 13, it is rejected applying as above rejecting claim 11, furthermore, Goertzel discloses the security level is based on the type of location determined for the network user node (Col 1, lines 10-65; remote access server, Internet, and mobile users; Col 5, lines 11-55; Col 6, lines 51-65; Intranet and extranet users in different locations, access levels assigned depending on locations and type of trust level/ access level assigned to it).

Regarding claim 15, it is rejected applying as above rejecting claim 11, furthermore, Goertzel discloses the step of modifying the security protection for the network user node includes a complete denial of access to information using the network user node (Fig 8, element 118: Security mechanism; Fig 12, element 1214: Deny access; Col 10, Lines 10- 52).

Regarding claim 16, it is rejected applying as above rejecting claim 11, furthermore, Goertzel discloses denial to a subset of the information accessible using the node(Col 10, lines 9-26; different level of access are assigned to different groups of users, some are denied all privileges, some are not; Col 12, lines 11-37; Col 16, lines 5-22; Fig 8, elements 124: restricted token, 118: security mechanism).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

4. Claims 3-10, 18-28, 30-33, 35-37, 38-48 are rejected under 35 USC 103 (a) as being unpatentable over Goertzel et al (Patent No: US 6308273 B1) in view of Bork et al (Patent No: US 6246376 B1).

Regarding claim 18, it is rejected applying as above rejecting claim 1, furthermore, Goertzel discloses a communication device capable of transmitting a data signal to the network user node containing instructions to modify the security protection for the node (Fig 6, element 88: Security provider, element 94: Access rights). Goertzel does not expressly disclose an input device, a processor, or a storage device connected to such system. However, Bork discloses an input device having a communicative coupling with a system for determining the location of a network user node (Col 8, Claim 1, lines 10-15); a storage device (Col 8, Claim 1, lines 15-30); a processor coupled to a storage device for processing information, storing on a storage device and generating a security modification instruction (Col 8, Claim 1, lines 10-15). At the time of the invention it would have been obvious to a person of ordinary skill in art to combine teachings of Bork with Goertzel to design a security system comprising an input device, a processor, and a storage medium. Motivation for doing so would have been to provide proper access rights and authentication for the mobile users (Bade, abstract; Page 1, paragraph [0009]).

Regarding claim 30, it recites the limitations of claim 18, therefore, it is rejected applying as above rejecting claim 18. Furthermore, Bork discloses security system comprising a memory coupled to the processor (Fig 3, element 302: ROM, element 306: RAM, element 304: data processor), and receiving location information using a network user node (Fig 3, element 104: GPS, element 112; Col 7, lines 25-55; GPS receiver; Col 9, claim 12; Bluetooth communication system). At the time of the invention it would have been obvious to a person of ordinary skill in art to combine teachings of Bork with Goertzel to design a security system further comprising a location information receiving step. Motivation for doing so would have been to provide proper access rights and

authentication for the mobile users and to facilitate such system with location information (Bade, abstract; Page 1, paragraph [0009]).

Regarding claim 38, it recites limitations of claims 1, and 18. Therefore, it is rejected applying as above rejecting claims 1, and 18.

Regarding claim 3, it is rejected applying as above rejecting claim 1, furthermore, Bork discloses the network user node's location is determined using a location sensing system (Col 2, Lines 39-67; Col 3, Lines 1-11; Col 8, Claims 1, 7, 8; remote indicator system, sensory output device). Goertzel and Bork are analogous art because they are from the same field of endeavor of maintaining network data security utilizing location information. At the time of the invention it would have been obvious to a person of ordinary skill in art to combine teachings of Bork with Goertzel to design a security system which uses a location sensing system (instead of IP address discrimination or Internet location services, Goertzel, Col 5, Lines 31-57) to locate user nodes. Motivation for doing so would have been simply to provide an alternative mechanism for determining trusted locations for mobile users (Goertzel, Col 1, and Col 2; Col 5, lines 25-30) or to determine user locations in high accuracy (Bork, Col 1, Col 2).

Regarding claim 4, it is rejected applying as above rejecting claim 3, furthermore, Bork discloses the location sensing system is a global positioning satellite (GPS) system (Col 2, Lines 39-67; Col 3, Lines 1-10; Col 4, Lines 28-52).

Regarding claim 5, it is rejected applying as above rejecting claim 3, furthermore, Bork discloses the location sensing system uses nearby access points to determine location (Col 2, Lines 39-67; Col 6, Lines 1-39; Col 7, Lines 7-55; Col 8, claim 1; Col 9, claim 12; Bork teaches using at least one GPS receiver antenna (array) to receive location data. Examiner interprets that such antenna usually is a part of wireless router or access point).

Regarding claim 6, it is rejected applying as above rejecting claim 3, furthermore, Bork discloses location sensing system uses signal bouncing and triangulation to determine network user node location (Col 2, Lines 39-67; Col 3, Lines 1-54; direction indicator devices using triangulation techniques; Col 6, Lines 17-37; Col 8, claim 1; Bork teaches wireless location and direction indicator system comprising use of GPS system, "BLUETOOTH" technique, signal receiving antenna, hopping sequence, and Geodetic Systems – examiner interprets such system usually includes signal bouncing to determine network users locations).

Regarding claim 7, it is rejected applying as above rejecting claim 3, furthermore, Bork discloses network user node is in direct communication with the location sensing system (Col 7, Lines 30-55; Col 6, Lines 1-16; Figure 3, element 112, 104, and 304; GPS receiver, signal receiving antenna).

Regarding claim 8, it is rejected applying as above rejecting claim 1, furthermore Bork discloses the steps of sending data signal includes transmitting the data signal using a wireless local area network (WLAN) protocol (Col 1, Lines 10-67; Col 2, Lines 5-37; wireless communication devices). At the time of invention, it will be obvious to a person with ordinary skill in the art to combine the teaching of Burk with Geotzel to design a method of adjusting security for wireless network in order to accurately measure the position of the users and to secure enterprise data from unwanted mobile user (Geotzel, Col 1, Lines 30-52; Bork, Col 1, Col 2).

Regarding claim 9, it is rejected applying as above rejecting claim 8, furthermore, Bork discloses WLAN protocol includes the IEEE 802.11 protocol (Col 1, Lines 10-67; Col 2, Lines 5-37; wireless communication devices; Col 8, claim 1, wireless location and direction indicator system. Burk does not disclose expressly IEEE 802.11 protocol, but because of such wide acceptance and use of IEEE 802.11 protocol in wireless networking, it is inherently clear that such protocol could be easily used in Burk's WLAN.

Regarding claim 10, it is rejected applying as above rejecting claim 8, furthermore, Bork discloses WLAN protocol includes Bluetooth wireless network protocol (Col 1, Lines 30-65; Col 2, Lines 5-37).

Regarding claim 26, it is rejected applying as above rejecting claims 11, and 18. Furthermore, Goertzel discloses selecting one access level from at least two of such access level (Col 19, claim 21; Col 20, claim 42), and a table containing access level and location information (Col 6, lines 51-65; Fig 6, element 92: location information (trust level)). Although Goertzel teaches IP addressing, and locations based on intranet and extranet, it does not expressly disclose GPS monitored physical locations. However, Bork discloses determining such physical locations of users through GPS system (Col 2, Lines 39-67; Col 3, Lines 1-11; Col 8, Claims 1, 7, 8; remote indicator system, sensory output device). At the time of the invention it would have been obvious to a person of ordinary skill in art to combine Bork's teachings of security system utilizing GPS monitored user locations with Goertzel's teachings of table comprising user locations and access level to design a system for modifying the security settings comprising the step of having a table stored on the storage device including user defined protection settings for a plurality of locations. Motivation for doing so would have been to provide an alternative mechanism for security and access controlling based upon users locations in a mobile/ wireless network.

Regarding claim 19, it is rejected applying as above rejecting claims 2, and 18.

Regarding claim 20, it is rejected applying as above rejecting claims 4, and 18.

Regarding claim 21, it is rejected applying as above rejecting claims 5, and 18.

Regarding claim 22, it is rejected applying as above rejecting claims 6, and 18.

Regarding claim 23, it is rejected applying as above rejecting claims 8, and 18.

Regarding claim 24, it is rejected applying as above rejecting claims 9, and 18.

Regarding claim 25, it is rejected applying as above rejecting claims 10, and 18.

Regarding claim 27, it is rejected applying as above rejecting claims 13, and 18.

Regarding claim 28, it is rejected applying as above rejecting claim 18.

Regarding claim 31, it is rejected applying as above rejecting claims 2, and 30.

Regarding claim 32, it is rejected applying as above rejecting claims 26, and 30.

Regarding claim 33, it is rejected applying as above rejecting claim 18, and 30.

Regarding claim 35, it is rejected applying as above rejecting claims 8, and 30.

Regarding claim 36, it is rejected applying as above rejecting claims 9, and 30.

Regarding claim 37, it is rejected applying as above rejecting claim 10, and 30.

Regarding claim 39, it is rejected applying as above rejecting claim 2, and 38.

Regarding claim 40, it is rejected applying as above rejecting claim 4, and 38.

Regarding claim 41, it is rejected applying as above rejecting claim 5, and 38.

Regarding claim 42, it is rejected applying as above rejecting claim 6, and 38.

Regarding claim 43, it is rejected applying as above rejecting claim 8, and 38.

Regarding claim 44, it is rejected applying as above rejecting claim 9, and 38.

Regarding claim 45, it is rejected applying as above rejecting claim 10, and 38.

Regarding claim 46, it is rejected applying as above rejecting claims 26, and 38.

Regarding claim 47, it is rejected applying as above rejecting claims 26, and 38.

Regarding claim 48, it is rejected applying as above rejecting claim 30, and 38.

5. Claims 14 is rejected under 35 USC 103 (a) as being unpatentable over Goertzel et al (Patent No: US 6308273 B1) in view of Bade et al (Publication No: US2002/0138632 A1).

Regarding claim 14, it is rejected applying as above rejecting claim 1, furthermore, Bade discloses the step of modifying the security protection for the network user node includes restricting access to information unless a password is properly entered (Page 2, Paragraph [0012],

[0021]; Page 3, Paragraph [0029]; special encrypted secret password). Goertzel and Bade are analogous art because they are from the same field of endeavor of maintaining network data security utilizing location information. At the time of the invention it would have been obvious to a person of ordinary skill in art to combine teachings of Bade with Goertzel to design a location based security/authentication system for mobile users in WAN environment. Motivation for doing so would have been to prevent unauthorized access in an extranet (Bade, Page 1, paragraph [0009]).

6. Claims 17, 29, 34, and 49 are rejected under 35 USC 103 (a) as being unpatentable over Goertzel et al (Patent No: US 6308273 B1) in view of Bork et al (Patent No: US 6246376 B1), further in view of Kennedy et al (Patent No:6084968).

Regarding claim 17, it is rejected applying as above rejecting claim 1, furthermore, Kennedy discloses the step of modifying the security protection for the network user node includes modifying data encryption parameters to change the strength of encryption on data transmitted by the network user node (Fig 7, element 101: selected encryption engine; Col 7, Claims 7, 10; different level of encryption). Goertzel and Kennedy are analogous art because they are from the same field of endeavor of providing data security in mobile communication network. At the time of the invention it would have been obvious to a person of ordinary skill in art to combine teachings of Kennedy with modified Goertzel- Bork system to design a security system with different level of encryption. Motivation for doing so would have been to provide strong data security and access control (Kennedy, Col 2, lines 41-46).

Regarding claim 29, it is rejected applying as above rejecting claims 17, and 18.

Regarding claim 34, it is rejected applying as above rejecting claims 17, and 30.

Regarding claim 49, it is rejected applying as above rejecting claims 17, and 38.

Conclusion

7. A shortened statutory period for response to this action is set to expire in 3 (Three) months and 0 (Zero) days from the mailing date of this letter. Failure to respond within the period for response will result in ABANDONMENT of the application (see 35 U.S.C 133, M.P.E.P 710.02(b)).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shanto Abedin whose telephone number is 571-272-3551. The examiner can normally be reached on M-F from 9:00 AM to 5:30 PM. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh, can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Shanto Abedin

Art Unit: 2136


AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100